KSI®

ORIGINAL

RECEIVED

FEB 10 1994

FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

9 February 1994

Mr. William F. Caton
Acting Secretary
Federal Communications Commission
Room 222
1919 M Street, N.W.
Washington, D.C. 20554

Re: CC Docket No. 93-292

Dear Mr. Caton:

This letter is KSI Inc.'s ("KSI") reply to comments in response to the above referenced docket regarding Policies and Rules concerning Toll Fraud.

KSI commends both the Commission and commentors such as McCaw Cellular Communications, Inc.(McCaw), The Cellular Telecommunications Industry Association (CTIA), and others regarding their stance on the seriousness of the industry-wide problem of cellular fraud Notice of Proposed Rulemaking (at para. 32) in general, and the importance of incorporating aids to combat wireless access fraud in particular. Clearly, as increasing percentages of the nation's communications (both voice and data) are carried over wireless systems such as cellular, PCS, and Personal Digital Assistants (PDAs), clone fraud will continue to ravage consumer and industry finances alike.

While we agree that the ability to manipulate ESNs must be significantly reduced by manufacturers, it is likely to be some time before major positive impacts can be felt. In addition, in excess of 14 million existing phones will necessarily remain unprotected. Although KSI agrees with the sentiment that positive steps to technologically reduce the ease by which a wireless device can be altered should be taken, criminals often have the resources required for sophisticated manipulation of wireless hardware and software. Fashioning additional rules or strengthening existing rules such as Rule 22-915 and/or attempts to enforce existing rules employ the basic premise that people will comply with rules. However, we know that those engaged in hardened criminal activity, such as drug-trafficking, will not in the least feel threatened by rules related to toll fraud. Just as we do not believe that handgun legislation will cause criminals to voluntarily give up their guns, we should not believe that rules and legislation regarding altering ESNs will deter most criminals from altering phones for fraudulent use. Opinions therefore arise which suggest that criminals can stay one step ahead of prosecution by Law Enforcement Agencies ("LEA").

While KSI believes that prevention is the best determent to fraud, we concur that fraudulent calling is often only a by-product of other crimes such as drug trafficking. In other words, wireless fraud is an integral part of many other illegal activities. Laws or rules do nothing to ensure detection of criminals. And detection of a crime without the ability to locate the fraudulent caller does nothing to strengthen enforcement. To stop those activities, the capability to locate and prosecute the criminal activity must be a known deterrent, incorporated into the system, and used.

No. of Copies rec'd 049
List ABCDE

KSI Inc. • 7630 Little River Turnpike • Suite 212 • Annandale, VA 22003 • (703) 941-5749 • Fax: (703) 941-5786

KSI is a corporation headquartered in Annandale, Virginia, with extensive experience and capability in developing systems which at their core employ location technology. Our patented Direction Finding Localization System ("DFLS") is a frequency-neutral RF location system, that through triangulation, determines the location of the wireless communication device. As mentioned in our correspondence of 30 December 1993 regarding docket 90-314, DFLS employs two major components: a network of local antenna signal processing subsystems called Support or Sensor Land Stations (SLSs) and a central control subsystem called a Control or Central Land Station (CLS). Directional measurements are extracted from wireless signals as they are received and processed by the SLSs. A control computer automatically provides position information suitable for display on a computer-based map. Although DFLS initially has been developed for use with cellular systems, the technology as stated above is frequency-neutral and will function in any wireless communications infrastructure that employs multiple base sites, including PCS. This solution can operate in a stand-alone mode or logically be integrated into the system equipment.

For less total cost than the carriers are losing annually, the top thirty (30) cities in the nation could have the major fraud prevention capability of DFLS. Once installed, DFLS can enable carriers in those cities to know much more quickly that fraud is being committed and allow them and the responsible LEAs to take action based upon that knowledge. In addition, those same cities would have wireless E-911 and a strong enabling technology for Intelligent Vehicle Highway Systems (IVHS) needs regarding incident detection and traffic flow, as well as other related services. One would argue that the economic savings of millions of dollars over weeks or months might be sufficient impetus for employing DFLS. However, KSI further agrees with commentors that more positive steps will likely be taken when the party that can best prevent the fraud, but doesn't, is assessed the cost of that fraud.

Thank you for the opportunity to submit this reply. If there are any questions on this submission, please contact the undersigned at (703) 941-5749.

Sincerely,

Charles J. Hinkle, Jr.
Director, Advanced Programs